

# IGC Group Organization Certificate Forms Packet

Copyright © 2017 IdenTrust Services, LLC. All rights reserved.

**Please verify these items are complete before submitting your paperwork.**

- Part 1 – Subscribing Organization Authorization Form** (see page 3)
  - All fields must be filled according to instructions.
  - Must be signed according to instructions.
  
- Part 2 – ID Form** (see page 5)
  - **Section 1: Terms and Conditions; Identity Credentials.** Information regarding identity credentials must be provided; must be signed in the presence of a notary (or other eligible Registrar)
  - **Section 2: Notarial (or other eligible Registrar) Acknowledgement.** Must be completed by notary of other eligible Registrar.

NOTE: instructions are provided on page 2.

## IGC Group Organization Certificate Instructions for Applying

### Instructions for Applicant

This form may be used to apply for Group Organization Certificate. Follow the Steps as provided below to apply. Unless otherwise defined on this page, capitalized terms have the meaning provided such term in Part 3 – IGC Group Organization Certificate Subscriber Agreement.

#### Step 1: Online Application

Complete the application process online.

#### Step 2: Subscribing Organization Authorization Form

Complete Part 1 – Subscribing Organization Authorization Form. Take Part 1 – Subscribing Organization Authorization Form to an officer of your Subscribing Organization (i.e. the entity named on in the "Subscribing Organization" field in Part 1 – Subscribing Organization Authorization Form) who can sign on behalf of your Subscribing Organization and bind your Subscribing Organization to the terms and conditions of Part 1 – Subscribing Organization Authorization Form. Have such officer sign Part 1 – Subscribing Organization Authorization Form and give you the signed original (i.e. signature in ink on paper) document for you to send to IdenTrust. In the event your Subscribing Organization does not have an "officer", then Part 1 – Subscribing Organization Authorization Form must be signed by an authorized representative of the Subscribing Organization with sufficient authority to bind the Subscribing Organization to the terms and conditions of Part 1 – Subscribing Organization Authorization Form.

#### Step 3: ID Form

Complete and Sign Part 2 – ID Form. Take Part 2 – ID Form to a notary (or other Registrar; "Registrar" is defined in Part 3 – IGC Group Organization Certificate Subscriber Agreement) to verify your identity credentials. Identity credentials used must be verifiable by IdenTrust. You have two options with respect to identity credentials used to complete Part 2 – ID Form:

- Option 1\*** – one U.S. Federal Government-issued photo identity credential (see BOX 1 below for examples); or
- Option 2** – two forms of identity credential issued by a state or local government, of which one of such two credentials must be a photo identity credential (see BOX 2 and BOX 3 below for examples).

##### Option 1\*

###### BOX 1 U.S. Federal Government-issued photo identity credential

- U.S. Passport
- Federal employee identity card
- US Military photo identity
- DoD CAC
- Certificate of US citizenship (must incorporate photo)

-OR-

##### Option 2

###### BOX 2 State or local government-issued photo identity credential

- State-issued Driver License
- State-issued identity card
- Student ID from a state college or university

###### BOX 3 Other acceptable forms of identity credential

- Original or certified copy of birth certificate
- Social Security card
- Concealed weapons permit
- State-issued pilot license

\*IdenTrust, in its sole discretion, may accept on a case-by-case basis photo identity credentials issued by a foreign national government with which the Federal Government of the United States of America has diplomatic relations. If you have questions as to whether your photo identity credential issued by a foreign national government is acceptable, please contact IdenTrust before you complete Part 2 – ID Form (contact information for IdenTrust is set forth at the bottom of this page).

Note: Please ensure that all information provided in Part 2 – ID Form matches the information you submitted in the online application, including all information about the "Subscriber" and "Subscribing Organization".

#### Step 4: Send Forms to IdenTrust

For your records, make a copy of the completed and signed Part 1 – Subscribing Organization Authorization Form and Part 2 – ID Form documents, then send the signed original (i.e. signature in ink on paper) documents to IdenTrust.

##### US Mail, FedEx, UPS, Etc.

IGC Registration  
IdenTrust Services, LLC  
5225 Wiley Post Way  
Suite 450  
Salt Lake City, UT 84116-2898

If you should have any questions during the process and would like to speak with a customer service representative, please call (800) 748-5360 or send an email to: [helpdesk@identrust.com](mailto:helpdesk@identrust.com)

## IGC Group Organization Certificate Part 1 – Subscribing Organization Authorization Form

This Subscribing Organization Authorization Form (the "Authorization") is given by "Subscribing Organization" (as identified below on this page), to IdenTrust Services, LLC, a Delaware corporation with its principal place of business located at 5225 Wiley Post Way, Suite 450, Salt Lake City, Utah 84116-2898 U.S.A ("IdenTrust").

WHEREAS, Subscribing Organization desires to authorize the issuance by IdenTrust of an IGC Group Organization Certificate (defined below) to Human Sponsor (identified below on this page) on behalf Subscribing Organization, that, if issued, will identify a Health Domain Name (defined below) as controlled or owned by Subscribing Organization and will certify the Public Keys (defined below) corresponding to such an IGC Group Organization Certificate.

WHEREAS, IdenTrust desires to receive this authorization and, if the application made by Human Sponsor corresponding to this Authorization is acceptable to IdenTrust, desires to issue an IGC Group Organization Certificate.

NOW, THEREFORE, Subscribing Organization and IdenTrust agree as set forth below.

1. The Subscribing Organization agrees to be bound by the terms and conditions of Schedule 1 hereto (attached hereto; see Part 1, Schedule 1 – Group Certificate Supplemental Terms) and the "IGC Group Organization Subscriber Certificate Agreement" (attached hereto; see Part 3 – IGC Group Organization Certificate Subscriber Agreement), and each of Schedule 1 and the IGC Group Organization Certificate Subscriber Agreement are incorporated herein by reference. Unless otherwise defined in this Authorization, capitalized terms used in this Authorization have the meaning given them under the IGC Group Organization Certificate Subscriber Agreement.
2. Subscribing Organization represents and warrants that Human Sponsor is an employee or authorized agent of Subscribing Organization. Subscribing Organization provides the information set forth in "Box 1" on this page to identify itself and Human Sponsor to IdenTrust.
3. Human Sponsor is hereby authorized by Subscribing Organization to represent the Subscribing Organization with respect to the application, issuance, acceptance, and use of an IGC Group Organization Certificate, including but not limited to use such IGC Group Organization Certificate to transact business and make Digital Signatures on behalf of the Subscribing Organization. Subscribing Organization hereby authorizes IdenTrust to issue an IGC Group Organization Certificate to Human Sponsor.
4. Subject to the provisions herein above and execution hereof by Subscribing Organization, IdenTrust accepts the authorizations made by Subscribing Organization herein above.

Subscribing Organization has caused this Authorization to be executed by an officer of Subscribing Organization or other authorized representative, effective on the date printed below. The person signing below on behalf of the Subscriber Organization personally represents and warrants that he or she has authority to accept the terms and conditions of this Authorization on behalf of Subscribing Organization and to bind the Subscribing Organization by his or her signature.

<p><b>Box 1</b></p> <hr/> <p>Name of Human Sponsor</p> <hr/> <p>Human Sponsor email address</p> <hr/> <p>Name of Subscribing Organization</p> <hr/> <p>Address of Subscribing Organization</p> <hr/> <p>Address line 2</p> <hr/> <p>City, State/Province, Postal Code</p>	<hr/> <p>Name of Subscribing Organization</p> <p>By: _____ (signature of organization officer/authorized representative)</p> <p>Name: _____</p> <p>Title: _____</p> <p>Date: _____</p>
---	--

**ALL FIELDS MUST BE COMPLETED**

## IGC Group Organization Certificate Part 1, Schedule 1 – Group Certificate Supplemental Terms

**1. Information Systems Security Officer.** The Subscribing Organization shall at all times during the term hereof have an Information Systems Security Officer. Subscribing Organization will identify to IdenTrust the then-current Information Systems Security Officer upon request from IdenTrust. IdenTrust may seek to verify the identity of the Information Systems Security Officer. IdenTrust is hereby authorized by Subscribing Organization to make inquiry with public or private databases or other sources, solely for the purpose of verifying any information provided regarding the identity of an Information Systems Security Officer provided by Sponsoring Organization in response to any request by IdenTrust. In the event that an Information Systems Security Officer's permission is necessary for IdenTrust to make such an inquiry, Sponsoring Organization shall be responsible for obtaining such permission and providing it to IdenTrust. IdenTrust also request Subscribing Organization to verify an Information Systems Security Officer's asserted affiliation with Subscribing Organization. IdenTrust is hereby also authorized to retain and use any information generated pursuant to the foregoing provisions of this Section, provided that such retention and use shall be subject to the terms of Section 12 the IGC Group Organization Certificate Subscriber Agreement.

**2. Responsibilities of the Information Systems Security Officer.** The Information Systems Security Officer shall be responsible for ensuring control of the Private Key of any IGC Group Organization Certificate issued pursuant to the Authorization, including maintaining a list of Human Sponsors who have access to or use of the Private Key on behalf of Subscriber, maintaining a list of Subscribers who have access to or use of the Private Key, and accounting for which Subscriber had control of the key at what time. IdenTrust designates Subscribing Organization as responsible for retaining the lists described in the immediately preceding sentence (the "Lists"), and Subscribing Organization agrees to retain the Lists. Subscribing Organization will provide to IdenTrust copies of the Lists: (i) upon request from IdenTrust; and (ii) upon termination hereof. The Information Systems Security Officer shall be responsible for ensuring compliance with the IGC Group Organization Certificate Subscriber Agreement by Subscribing Organization in relation to use and administration of any IGC Group Organization Certificate issued pursuant to the Authorization; provided, however, in no event shall the foregoing provisions of this sentence be deemed or construed to reduce the responsibility of Subscribing Organization with respect to fulfilling its duties and obligations under the IGC Group Organization Certificate Subscriber Agreement.

**3. Initial Subscriber.** The Human Sponsor identified to IdenTrust by Sponsoring Organization in the Authorization to which this Schedule 1 is attached shall be the only Human Sponsor to act on behalf of Subscriber with respect to accessing the IdenTrust online systems in relation to the administration of Certificate lifecycle events (e.g. application, issuance, renewal) with IdenTrust (such Human Sponsor, the "Initial HS"); provided, however, Sponsoring Organization may replace the Human Sponsor who is the Initial HS by making a change pursuant to Section 12 of the IGC Group Organization Certificate Subscriber Agreement.

**4. Additional Subscribers.** Exclusive of the Initial HS and any replacement thereof by another Human Sponsor as described in Section 3, Sponsoring Organization may authorize other Human Sponsors to use and administer on behalf of Subscribing Customer the Certificate as provided under the IGC Group Organization Certificate Subscriber Agreement, exclusive of its Section 12, provided that for each such other Human Sponsor the Subscribing Organization:

- (i) verifies and records the information required under Section 3.2.3.3 of the CPS relative to "Group Organizational Certificate" (as such term is used in such Section); and
- (ii) obtains and records written agreement of each such other Human Sponsor to the terms applicable to "You" and "Human Sponsor" under the IGC Group Organization Certificate Subscriber Agreement.

**5. Representation and Warranty – subjectNameDN.** Subscribing Organization represents and warrants that the information provided in connection with the application process related to the Certificate for use in as the "subjectName DN" field within the Certificate does not imply that the subject is a single individual (e.g. by inclusion of a human name form).

**6. Representation and Warranty – HIPPA.** Subscribing Organization represents and warrants that it is qualified in one of the following categories:

- (iii) HIPPA Covered Entity;
- (iv) HIPPA Business Associate; or
- (v) Healthcare-related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPPA.

**7. Definitions.** Unless otherwise defined in this Schedule 1, capitalized terms used in this Schedule 1 have the meaning given them under the Authorization to which this Schedule 1 is attached.

"HIPPA" means the Health Insurance Portability and Accountability Act of 1996, as has been amended from time to time, including but not limited to amendments made under the Health Information Technology for Economic and Clinical Health Act of 2009.

"HIPPA Business Associate" means a "Business Associate" as defined in HIPPA.

"HIPPA Covered Entity" means a "Covered Entity" as defined in HIPPA.

"Information Systems Security Officer" means an individual responsible for establishing and maintaining the enterprise vision, strategy, and program as it relates to information systems security, to ensure information assets are adequately protected.

## IGC Group Organization Certificate Part 2 – ID Form

**Section 1: Terms and Conditions; Identity Credentials**

The undersigned in this Section 1 warrants and represents that all facts and information provided in Part 1 – Subscribing Organization Authorization Form and this Part 2 – ID Form are, to the best of the undersigned’s knowledge, accurate, current, and complete, and that he or she: (i) is authorized by his or her Subscribing Organization (as identified on the Part 1 – Subscribing Organization Authorization Form naming him or her as "Human Sponsor" in connection with the application made for a digital certificate in connection with this Part 2 – ID Form) to apply for, be issued, accept, and use an IGC Group Organization Certificate issued by IdenTrust; (ii) has reviewed and accepts as identifying himself or herself the personal identifying information set forth below on this Part 2 – ID Form; (iii) is who he or she represents himself or herself to be; and (iv) has read, understands, and accepts the terms and conditions set forth in Part 3 – IGC Group Organization Certificate Subscriber Agreement.

Sign below in this Section 1 only in the presence of a notary (or other Registrar; "Registrar" is defined in Part 3 – IGC Group Organization Certificate Subscriber Agreement). If this Section 1 is signed within the United States, the signer makes the following declaration by doing so: I declare under penalty of perjury that the foregoing is true and correct. If this Section 1 is signed without (i.e. outside of) the United States, this signer makes the following declaration by doing so: I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

\_\_\_\_\_  
(signature of Human Sponsor)

\_\_\_\_\_  
(print email address of Human Sponsor)

\_\_\_\_\_  
(print first, middle, and last name of Human Sponsor)

**See accompanying instructions for more information regarding acceptable forms of identity credentials. Non-U.S. identity credentials used in BOX 1 must be IdenTrust-approved in advance. All fields must be completed.**

**BOX 1: U.S. Federal Government photo identity credential (for non-U.S. credentials see instructions).**

**Photo ID**

Doc. Type/Title: \_\_\_\_\_  
 Doc. Issuer: \_\_\_\_\_  
 Serial/Unique #: \_\_\_\_\_  
 Exact Name: \_\_\_\_\_  
 Issue Date: \_\_\_\_\_  
 Expiration Date: \_\_\_\_\_

-OR-

**BOX 2 and BOX 3: State or local government-issued photo identity credential AND one other acceptable form of identity credential.**

**Photo ID**

Doc. Type/Title: \_\_\_\_\_  
 Doc. Issuer: \_\_\_\_\_  
 Serial/Unique #: \_\_\_\_\_  
 Exact Name: \_\_\_\_\_  
 Issue Date: \_\_\_\_\_  
 Expiration Date: \_\_\_\_\_

**Second ID**

Doc. Type/Title: \_\_\_\_\_  
 Doc. Issuer: \_\_\_\_\_  
 Serial/Unique #: \_\_\_\_\_  
 Exact Name: \_\_\_\_\_  
 Issue Date: \_\_\_\_\_  
 Expiration Date: \_\_\_\_\_

**Note:** If the name on the photo identity credential is different from the name on the second identity credential, IdenTrust may request from Human Sponsor a notarized copy of a document showing the name change (e.g. a notarized copy of marriage license, notarized certificate of marriage).

**Section 2: Notarial (or other eligible Registrar) Acknowledgement**

I, \_\_\_\_\_ registered in (if notary) / resident of (if other Registrar than notary) in the state of \_\_\_\_\_, county of \_\_\_\_\_ do hereby certify under PENALTY OF PERJURY under the laws of such state that the following information is true and correct:

- (a) On \_\_\_\_/\_\_\_\_/\_\_\_\_ (MM/DD/YY), before me personally appeared \_\_\_\_\_ (name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.
- (b) I have seen and verified the forms of identification for which information is written above and hereby assert that said forms of identification do not appear to be altered, forged, or modified in any way.

WITNESS my hand and, if this Section 2 is executed by a notary, official seal.

\_\_\_\_\_  
(signature)

(Seal)

## PART 3 – IGC GROUP ORGANIZATION CERTIFICATE SUBSCRIBER AGREEMENT

This IGC Group Organization Certificate Subscriber Agreement (this "Agreement") is made by and among IdenTrust (defined below) on the one hand, and You (defined below) and Subscribing Organization (defined below) on the other. This Agreement sets the forth terms and conditions governing Your (defined below) application for a Certificate (defined below) and, if IdenTrust issues such Certificate to You, the terms and conditions applicable to the Certificate. Definitions of capitalized terms used herein are provided for in Section 36 below.

- 1. Acceptance.** By signing the ID Form referencing this Agreement or by clicking the checkbox next to "I have reviewed, and I hereby sign and accept the complete terms of the Subscriber Agreement" during the online application process linking to this Agreement, You agree to the terms and conditions of this Agreement. It is understood that the Human Sponsor is responsible for the operation and control of You, and the Human Sponsor assumes the duties and obligations of You with respect to the Certificate hereunder. Subscribing Organization indicates its acceptance to the provisions hereof through the execution of the Subscribing Organization Authorization Form under which You are identified by the Subscribing Organization as affiliated therewith for purposes of the Certificate. If IdenTrust accepts the application and confirms the information submitted, IdenTrust will create the Certificate in the name of Subscribing Organization (i.e. to be identified in within the "subject:organizationName" field of the Certificate) and the Health Domain Name provided by You in the application, and will notify You how and where to retrieve the Certificate.
- 2. Integration; Amendment.** The CP, CPS, ID Form, and Subscribing Organization Authorization Form are incorporated by reference herein. The parties hereto agree that the CP and CPS can be amended from time to time by IdenTrust pursuant to the terms regarding amendment thereof set forth in the CP and CPS, respectively, and that any such amendments shall become effective as set forth in the CP and CPS, respectively. The terms of this Agreement may be amended upon renewal of the Certificate by the parties hereto with effect of such amendment at the time of such renewal, or at any time by IdenTrust with effect thirty (30) days after IdenTrust posts amended terms to the Repository. Use of the Certificate after the effective date of any such amendment shall constitute notice to IdenTrust of acceptance by Subscribing Organization and You of the amended terms; You may decline to accept any such amended terms by refraining from using the Certificate after the effective date of the applicable amendment. Subscribing Organization and You are responsible for periodically checking the Repository for the latest version of the CP, CPS, and this Agreement.
- 3. Application.** You must complete both the online portion of the application process and provide to IdenTrust the Subscribing Organization Authorization Form and ID Form. The identity credentials You presented and which were recorded on the ID Form must be the same identity credentials as those reported to IdenTrust during the online portion of the application process.
- 4. Verification of Identity.** IdenTrust may seek to verify the identity and existence of You and that of the Subscribing Organization by any reasonable means. IdenTrust is hereby authorized by You and Subscribing Organization, as applicable, to make inquiry with public or private databases or other sources, solely for the purpose of verifying any information that You or Subscribing Organization provide during the application process in order to determine whether to issue a Certificate to the You. IdenTrust may contact Subscribing Organization's to verify Your affiliation with Subscribing Organization. IdenTrust is hereby also authorized to retain and use any information generated during the application, identification, authentication, Certificate issuance, and Certificate management processes, provided that such retention and use shall be subject to the terms of this Agreement, including but not limited to Section 12.
- 5. Processing Payment.** IdenTrust will begin processing the application for a Certificate made in connection herewith as soon as IdenTrust has received the following in connection herewith: (i) preauthorization to charge the credit card, purchase order, or voucher number provided by You; and (ii) the Subscribing Organization Authorization Form and the ID Form. You and Subscribing Organization, as may be applicable, hereby authorize IdenTrust to bill against such credit card, purchase order, or voucher number for the applicable Certificate issuance fee. In the event IdenTrust approves Your application for a Certificate in connection herewith, IdenTrust will process the credit card charge, purchase order, or voucher number. Once such processing occurs, unless otherwise required by law, no refunds will be provided by IdenTrust. If a Certificate is issued to You hereunder, IdenTrust will revoke the Certificate if IdenTrust does not actually receive payment for the Certificate within sixty (60) days of such issuance.
- 6. Approval of Application by IdenTrust.**

IdenTrust, in its sole discretion and without incurring liability for any loss arising out of such denial or refusal, may deny the application for, or otherwise refuse to issue, an Certificate in connection herewith. IdenTrust shall have no liability for any delay experienced during the Certificate application and issuance process.

If IdenTrust approves the application for a Certificate made in connection herewith, notice thereof will be provided as describe in Section 7 and the certificate will be made available to issuance in keeping with the applicable provisions of Section 7 – 9, as applicable.

If IdenTrust does not approve Your application for a Certificate in connection herewith, IdenTrust will send notice of such non-approval to the email address listed for Human Sponsor on the ID Form and upon the sending of such a notice this Agreement terminates.

### 7. Certificate Issuance – Notice and Time to Download.

If IdenTrust approves the application for a Certificate made in connection herewith, IdenTrust will notice You that the Certificate is ready to be so issued. To so notice You, IdenTrust will email You at the email address for Human Sponsor as identified to IdenTrust on the ID Form. If IdenTrust sends You such notice, You must download the corresponding Certificate from the Web site specified by IdenTrust in the email within thirty (30) days of the completion date of the ID Form (i.e. the date provided on the ID Form with Your signature) that was part of the approved application for such Certificate. If such download has not occurred within such thirty (30) day

period, the ID Form becomes invalid and void for the purposes of applying for and issuing a Certificate, and the associated approval by IdenTrust will become void and this Agreement shall terminate without any refund of fees being payable by IdenTrust.

#### **8. Cryptomodule Requirement.**

You must have and activate a Cryptomodule in order to download the Certificate. IdenTrust will provide You with instructions regarding such activation in connection with IdenTrust noticing You that issuance of the Certificate to You has been approved. Further, with respect to the Cryptomodule that You use in connection with the Certificate, You agree:

- (i) to protect from disclosure to any other person Your password or other data used to activate the Cryptomodule (except any person that Subscribing Organization expressly identifies to you as an Additional Subscriber);
- (ii) not to leave the Cryptomodule unattended or open to unauthorized access while it is active; and
- (iii) deactivate the Cryptomodule by manual logout or by use of an inactivity timeout function effecting automatic logout.

You (and not IdenTrust) are responsible for providing the Cryptomodule that You will use, for its ability to be used with the Certificate, and for its compliance with the applicable requirements of the CP and CPS.

#### **9. Certificate Issuance – Review of Certificate Contents, Downloading, and Acceptance of Certificate.**

Prior to the Certificate being made available to You for downloading as described in Section 7, the contents of the Certificate shall be made available to You for review and You hereby agree that You shall review such contents. The contents of the Certificate will be based on information provided by You and the Subscribing Organization during the application process, including but not limited to information provided on Your behalf by Human Sponsor during the online application process as well as information provided on the Subscribing Organization Authorization Form and ID Form. If upon Your review of the Certificate contents You determine the any portion of the content of the Certificate is not accurate or valid, You hereby agree that You shall not download the Certificate and You shall instead immediately inform IdenTrust of the inaccurate or invalid portion(s) by contacting the IdenTrust Help Desk by phone at 1-800-748-5360 or by email at helpdesk@IdenTrust.com.

By downloading the Certificate after its contents are made available for Your review as described above, You accept the Certificate, warrant the accuracy and validity of its contents, and reaffirm Your acceptance of the terms of this Agreement (including but not limited to each of the representations and warranties You make under this Agreement). Without limiting the foregoing, Your failure to object to the Certificate or its contents by informing IdenTrust of such objection within twenty-four (24) hours of downloading it constitutes acceptance of the Certificate by You and Subscribing Organization. Notwithstanding the foregoing provisions of this paragraph, any use by You of the Certificate constitutes acceptance of the Certificate by You and Subscribing Organization.

**10. Declaration of Identity.** In the event that IdenTrust issues a Certificate to You in connection herewith, You agree that IdenTrust may require You to provide a declaration of Your identity information on a form provide by IdenTrust and require such declaration be digitally signed by You using such Certificate. In the event that You do not so sign such declaration when provided by IdenTrust, it is understood that IdenTrust will revoke the Certificate.

**11. Legal Effect of Digital Signatures.** All Digital Transmissions that are signed with a Digital Signature by You using a Private Key corresponding to the Certificate shall have the same legal effect, validity, and enforceability as if the Digital Transmissions had been in writing and manually signed by You. Neither You nor Subscribing Organization will challenge the legal effect, validity, or enforceability of a Digital Transmission on the basis of such Digital Transmission being in digital, rather than in written, form. You and Subscribing Organization shall be responsible for all Digital Transmissions that are Digitally Signed by You using a Private Key corresponding to the Certificate.

**12. Privacy.** IdenTrust agrees to use reasonable care to safeguard personally identifying information about You obtained by IdenTrust during the application, identification and authentication, and Certificate issuance processes, as well as in the course of communications between You and IdenTrust made in connection with the Certificate during the Validity Period of the Certificate. Use by IdenTrust of such personally identifying information shall be limited to use as provided for under this Agreement, the CPS, the IdenTrust Privacy Policy, or by You in writing. You hereby authorize IdenTrust to contact You and Subscribing Organization with information and offers from IdenTrust related to renewals of the Certificate. You also hereby authorize IdenTrust to disclose information about You to Subscribing Organization in connection with use and administration of the Certificate.

Notwithstanding the foregoing, information contained in the Certificate and information about the status of the Certificate is not private; treating such information as private would defeat the purpose of the Certificate, which is to establish Your identity. Accordingly, IdenTrust may disclose without limitation, save for any limitations on the disclosure of such information that may set forth in the CP or CPS any information contained in any of the Certificate, CRLs, OCSP responses, or the LDAP directory, including but not limited to the Public Keys, email addresses, Subscribing Organization's name, the certificate serial number, Certificate expiration date, and Certificate status such as valid, invalid, revoked, or expired.

**13. Term.** Certificates will be valid for the Validity Period specified therein unless revoked as provided for herein prior to the end of such period. The term of this Agreement shall correspond to the term of the Certificate's validity. Sections 12, 13, 17 (insofar as the provisions thereof requiring You to "cease using the Certificate"), 21 – 36 of this Agreement will survive the termination, expiration, or revocation of this Agreement or the Certificate.

#### **14. Permitted Uses of the Certificate.**

The Certificate may be used for authentication, for Access Controls, to create Digital Signatures, to support verification of Digital Signatures, to achieve confidentiality through the use of encipherment of shared secret, provided such use is consistent with the use described in the "Key usage extension" and "extended Key usage extension" in the Certificate.

The Group Organization Signing Certificate issued in connection herewith may be used in applications where: (i) the identity of communicating parties needs to be authenticated; (ii) a message or file needs to be bound to the identity of its originator by a signature (i.e. You); or (iii) the integrity of the message or file has to be assured.

The Group Organization Encryption Certificate issued in connection herewith may be used in applications where a message or file needs to be protected against disclosure to anyone else except You and intended recipients.

**15. Change in Human Sponsor.** Subscribing Organization may change its employee(s) or agent(s) who are authorized to use and administer on behalf of Subscribing Customer the Certificate as provided for hereunder, without requesting revocation of the current Certificate, provided that Subscribing Organization shall bear the security and control risks associated with making such changes without revoking the Certificate. Such change may be effected by Subscribing Organization's execution of the then-current form of Subscribing Organization Authorization Form and submission of the then-current form ID Form completed by such employee or agent.

**16. Prohibited Uses of the Certificate.** Notwithstanding any other provision hereof, the Certificate must not be used for:

- (i) any application requiring fail-safe performance such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system whose failure could lead to injury, death or environmental damage;
- (ii) transactions where applicable law prohibits the use of Certificates for such transactions or where otherwise prohibited by law;
- (iii) to present, send or otherwise transfer hostile code, including spyware or other malicious software; or
- (iv) to issue any other Certificate.

**17. Your General Obligations.**

You agree:

- (i) to accurately represent You in all communications with IdenTrust;
- (ii) to protect the Private Keys corresponding the Certificate that You are issued in connection herewith, including by not limited to protecting them from access by third parties (other than persons designated by Subscribing Organization as provided in the Subscribing Organization Authorization Form and in conformity with the applicable requirements of the CP and CPS;
- (iii) that You and Subscribing Organization assume all risk of any use of Your Private Key(s) or Certificates in violation of this Agreement; and
- (iv) to respond within twelve (12) hours to IGC-related notices issued by IdenTrust relating to actual or possible compromise of a Private Key corresponding to the Certificate or misuse of the Certificate.

You must request that the Certificate be revoked:

- (i) within one hour of You first suspecting or discovering that a Private Key corresponding to a Public Key listed in the Certificate is compromised; or
- (ii) within 24 hours of You of any information in the Certificate relating to Your identity, Your affiliation with Subscribing Organization no longer being valid, accurate, current or complete, or becomes misleading.

You may request that the Certificate be revoked at any time for reasons other than those described above in this Section 17.

You must immediately cease using the Certificate in the following circumstances:

- (i) when You suspect or discover that the Private Key corresponding to the Certificate is compromised;
- (ii) when any information in the Certificate is no longer accurate, current, or complete, or such information becomes misleading;
- (iii) upon the revocation or expiration of the Certificate; or
- (iv) upon termination of this Agreement.

In the event You have applied for a type of Certificate that includes "Hardware" in its title and IdenTrust approves the issuance of such Certificate to You, You agree:

- (i) that You will protect all passwords and personal identification numbers used to access the Cryptomodule corresponding to the Certificate; and
- (ii) that the Private Keys corresponding to the Certificate that corresponds to the Cryptomodule never exist in plain text outside the Cryptomodule.

**18. Subscribing Organizations Direct Revocation Responsibilities.** Subscribing Organization agrees that it shall immediately request that IdenTrust revoke the Certificate and require You to cease use of the Certificate, if there is no longer a Human Sponsor corresponding to the Certificate. Also, Subscribing Organization may request revocation of the Certificate at any time.

**19. Revocation Requests by You or Subscribing Organization.**

You or Subscribing Organization can request revocation of the Certificate by:

- (i) sending an email that is signed by You using the Private Key corresponding to the Certificate that You are requesting be revoked to helpdesk@IdenTrust.com;
- (ii) calling the IdenTrust Help Desk at 1-800-748-5360;
- (iii) online-request via IdenTrust's online certificate management interface systems, if such systems are made available to You and You has signed up for access to such IdenTrust online systems, which such availability and access, if any, are outside the scope of this agreement; or



- (iv) such other means as may be provided to You by IdenTrust.

**20. Revocation of the Certificate by IdenTrust.** IdenTrust may revoke the Certificate without notice to You for any reason provided under the CPS. Unless prohibited by law or government rule, regulation, or order, in the event IdenTrust revokes the Certificate under this Section 20, IdenTrust shall use commercially reasonable efforts to promptly notify You of the action taken. Additionally, upon receiving a request for revocation of the Certificate, IdenTrust will promptly revoke the Certificate after determining the request was made by a person authorized to do so or if IdenTrust otherwise determines the Certificate should be revoked. Once a Certificate has been revoked, it cannot be used or reinstated. In the event that the a voucher number was billed against as provided for in Section 5, IdenTrust can revoke the Certificate if the entity that paid IdenTrust for such voucher requests IdenTrust to do so.

**21. Representations, Warranties, and Covenants from You.**

You represent and warrant to IdenTrust that:

- (i) all information provided by You (and the Subscribing Organization) that is included in the Certificate and all representations made by You in connection with Your application for the Certificate, are true and not misleading;
- (ii) each Digital Signature created using the Private Key corresponding to the Public Key listed in the Group Organization Signing Certificate is a Digital Signature by You;
- (iii) the Private Keys corresponding to the Public Keys listed in the Certificate have been protected continuously since You generated them during the issuance process of the Certificate and that no unauthorized person has had access to such Private Keys;
- (iv) the Certificate and the corresponding Key Pair will and are, as applicable, being used exclusively for purposes that are authorized by the Subscribing Organization and under the CP and CPS and that are legal; and
- (v) the Subscribing Organization name and Health Domain Name in the Certificate are accurate, current, complete, and not misleading.

Such representations and warranties shall survive the termination hereof, but shall only apply with respect to the Certificate as it stood during its Validity Period.

You covenant to IdenTrust that:

- (i) You will accurately represent his or herself in all communications with IdenTrust;
- (ii) You will protect the Private Keys corresponding the Certificate that You are issued in connection herewith, including by not limited to protecting such Private Keys from access by third parties and in conformity with the applicable requirements of the CP and CPS; and
- (iii) You will use the Private Keys corresponding to any Certificate that You are issued in connection herewith only uses allowed herein, under the CP, and Section 1.4 of the CPS.

**22. Indemnification by You.**

You agree to indemnify and hold harmless each PKI Service Provider (including but not limited to IdenTrust), its affiliates, and their respective directors, officers and employees for any and all loss, cost, damage, or expense (including reasonable attorneys' fees and expenses) that arises from or relates to Your:

- (i) improper use of the Certificate or Key Pairs;
- (ii) failure to safeguard Private Keys;
- (iii) failure to comply with the provisions of the CP, the CPS, or this Agreement,
- (iv) breach of any representation or warranty made by You hereunder, or
- (v) acts or omissions giving rise to a loss by any PKI Service Provider.

For purposes of the foregoing provisions of this Section 22, each PKI Service Provider other than IdenTrust is a third party beneficiary.

**23. Representations, Warranties, and Covenants from Subscribing Organization.**

Subscribing Organization:

- (i) represents and warrants that it authorizes the affiliation of You with Subscribing Organization for the Certificate, as such affiliation is described under the CP and CPS;
- (ii) represents and warrants that any information that it may provide in connection with the application process related to the Certificate, including but not limited to identity information, is accurate, current, and complete;
- (iii) represents and warrants that it is duly-organized and validly-existing under the laws of its state of organization, to perform all duties and obligations of Subscribing Organization;
- (iv) has full right and authority to use for purposes of identifying Subscribing Organization in the Certificate the Subscribing Organization's name and the Health Domain Name provided by the Human Sponsor to IdenTrust during the application process;
- (v) represents and warrants that the Human Sponsor(s) identified as provided for in the Subscribing Organization Authorization Form or as otherwise appointed by Subscribing Organization pursuant to Section 15 is employed by or is the authorized agent of Subscribing Organization, and is authorized to act on behalf of Subscribing Organization in all respects related to and in connection with the Certificate;
- (vi) covenants that it will immediately request revocation of the Certificate by IdenTrust if (a) information contained in the Certificate is no longer accurate or current, or (b) the Health Domain Name that You provided for inclusion in the Certificate is no longer owned or controlled by the Subscribing Organization, (c) You are no longer authorized by Subscribing Organization to transact business or make Digital Signatures on behalf of Subscribing Organization; (d) has no Human Sponsor designated for You.

Such representations, warranties, and covenants shall survive the termination hereof, but shall only apply with respect to the Certificate as it stood during its Validity Period.

**24. Indemnification by Subscribing Organization.**

Subscribing Organization agrees to indemnify and hold harmless IdenTrust, its affiliates, and their respective directors, officers and employees from any and all loss, cost, damage, or expense (including reasonable attorneys' fees and expenses) arising from or related to:

- (i) any misrepresentation or omission of material fact made by Subscribing Organization or You to IdenTrust;
- (ii) any breach of this Agreement, the CP, or the CPS by Subscribing Organization or You; or
- (iii) any misuse of the Certificate (other than by IdenTrust).

In the event Subscribing Organization is a Government Agency, then Subscribing Organization's obligation to indemnify and hold harmless under the provisions above in this Section 24 are reduced to the extent necessary to comply with the requirements of federal law of the United States of America if the Government Agency is a government body or administrative unit of the Federal Government of the United States of America or the law of the applicable State which the Government Agency is a government body or administrative unit among the United States of America which limits or prohibits Your indemnification other entities.

**25. IdenTrust Representations and Warranties.**

IdenTrust provides the representations and warranties set forth in Section 9.6.1 of the CPS to the extent such are applicable with respect to the Certificate that is the subject of this Agreement. Such representations and warranties shall survive the termination hereof, but shall only apply with respect to the Certificate as it stood during its Validity Period.

**26. Disclaimer of Warranties; Limitations on Liability.**

EXCEPT FOR THE REPRESENTATIONS AND WARRANTIES EXPRESSLY PROVIDED BY IDENTRUST ABOVE IN SECTION 25, IDENTRUST DISCLAIMS ANY AND ALL OTHER WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO ANY SERVICES OF IDENTRUST PROVIDED IN CONNECTION HERewith OR THE CERTIFICATE. IDENTRUST MAKES NO WARRANTY REGARDING THE CONTENT OF ANY WEBSITE OR SERVER USING THE CERTIFICATE.

IDENTRUST SHALL HAVE NO LIABILITY: (I) FOR LOSS DUE TO USE OF THE CERTIFICATE, UNLESS THE LOSS IS PROVEN TO BE A DIRECT RESULT OF A BREACH BY IDENTRUST OF THIS AGREEMENT OR THE CPS OR A PROXIMATE RESULT OF THE GROSS NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT OF IDENTRUST. IDENTRUST SHALL HAVE NO LIABILITY FOR CLAIMS ALLEGING ORDINARY NEGLIGENCE; OR (II) IF IDENTRUST IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITTS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF ANY PROVISION OF ANY APPLICABLE LAW, REGULATION, OR ORDER, THE FAILURE OF ANY ELECTRICAL, COMMUNICATION, OR OTHER SYSTEM OPERATED BY ANY PARTY OTHER THAN IDENTRUST OR ANY ACT OF GOD, EMERGENCY CONDITION OR WAR OR OTHER CIRCUMSTANCE BEYOND THE CONTROL OF IDENTRUST.

NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER IDENTRUST NOR ANY PKI SERVICE PROVIDER SHALL HAVE ANY LIABILITY ARISING FROM IMPROPERLY USED OR IMPROPERLY RELIED UPON CERTIFICATES.

IN NO EVENT SHALL IDENTRUST'S TOTAL, AGGREGATE LIABILITY UNDER THIS AGREEMENT EXCEED AN AMOUNT EQUAL TO THE ACTUAL AMOUNT PAID TO IDENTRUST FOR ISSUANCE OF THE CERTIFICATE TO YOU HEREUNDER.

NOTWITHSTANDING ANY OTHER PROVISION HEREOF AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL IDENTRUST BE LIABLE FOR ANY EXEMPLARY, PUNITIVE, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, ANY LOSS OF PROFITS, LOSS OF DATA, OR COST OF PROCUREMENT OF SUBSTITUTE SERVICES, HOWEVER CAUSED, AND ON ANY THEORY OF LIABILITY, WHETHER FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), OR OTHERWISE. THE FOREGOING LIMITATIONS WILL APPLY WHETHER OR NOT IDENTRUST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER OR NOT IDENTRUST COULD HAVE FORESEEN SUCH DAMAGES, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

EACH PARTY HERETO UNDERSTANDS THAT THE FOREGOING LIMITATION OF LIABILITY AND RECOURSE IS AN ESSENTIAL INDUCEMENT TO IDENTRUST TO ENTER INTO THIS AGREEMENT AND PROVIDE THE SERVICES.

**27. Dispute Resolution.**

In the event of any dispute or disagreement between the parties hereto ("Disputing Parties") arising out of or related to this Agreement or the Server Certificate, the Disputing Parties will use their best efforts to settle the dispute or disagreement through mediation or good faith negotiations following notice from one Disputing Party to the other. If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice, then the Disputing Parties will submit the dispute to binding arbitration, as provided below.

Except for a controversy, claim, or dispute involving the Federal Government of the United States or a "Core Proceeding" under the United States Bankruptcy Code, the parties agree to submit any controversy, claim, or dispute, whether in tort, contract, or otherwise arising out of or related in any way to this Agreement, that cannot be resolved by mediation or negotiations between the parties, for resolution by binding arbitration by a single arbitrator, and judgment upon the award rendered by the arbitrator may be entered in any court having jurisdiction over the parties. The arbitrator will have no authority to impose penalties or award punitive damages. Binding

arbitration will: (i) proceed in New York County, New York; (ii) be governed by the Federal Arbitration Act (Title 9 of the United States Code); and (iii) be conducted in accordance with the Commercial Arbitration rules of the American Arbitration Association ("AAA"). Each party will bear its costs for the arbitration; however, upon award of any judgment or conclusion of arbitration, the arbitrator will award the prevailing party the costs it expended in such arbitration. Unless the arbitrator otherwise directs, the parties, their representatives, other participants, and the arbitrator will hold the existence, content, and result of the arbitration in confidence. This arbitration requirement does not limit the right of any party to obtain provisional ancillary remedies such as injunctive relief or the appointment of a receiver, before, during, or after the pendency of any arbitration proceeding. This exclusion does not constitute a waiver of the right or obligation of any party to submit any dispute to arbitration.

**28. Choice of Law; Conflicts.** Subject to any limits appearing in applicable law, the laws of the state of New York, U.S.A., shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions. If any provision of this Agreement is found to be invalid or unenforceable, then this Agreement shall be deemed amended by modifying such provision to the extent necessary to make it valid and enforceable while preserving its intent or, if that is not possible, by striking the provision and enforcing the remainder of this Agreement.

**29. Assignment.** Neither You nor Subscribing Organization will assign any of their rights or obligations under this Agreement without the written consent of IdenTrust. Any assignment in violation of the foregoing sentence shall be null and void.

**30. Third Party Beneficiaries.** Each Relying Party is an intended third party beneficiary of each representation, warranty, and covenant made by any of Subscribing Organization or You hereunder.

**31. Relationship Of The Parties.** Nothing in this Agreement shall be deemed to create a partnership or joint venture or fiduciary relationship between IdenTrust and any other party, nor make another party the agent, partner, employee, or representative of IdenTrust.

**32. Headings And Titles.** The headings and titles contained in this Agreement are included for convenience only, and will not limit or otherwise affect the terms of this Agreement.

**33. Waiver.** No waiver by either party of any default will operate as a waiver of any other default, or of a similar default on a future occasion. No waiver of any term or condition by any party will be effective unless in writing and signed by the party against whom enforcement of such waiver is sought.

**34. Severability.** In case one or more of the provisions of this Agreement should be held invalid, illegal or unenforceable in any respect for any reason, the same will not affect any other provision in this Agreement, which will be construed to give maximum effect to the extent of the parties as evidenced by this original Agreement as originally drafted save to the extent of such invalid, illegal or unenforceable provision.

**35. Entire Agreement.** This Agreement represents the entire agreement of the parties, and supercedes all other agreements and discussions relating to the subject matter hereof. Except as expressly provided otherwise in this Agreement, this Agreement may not be amended except in writing signed by the parties.

**36. Definitions.** Unless otherwise defined below, capitalized terms used in this Agreement have the meaning given them in the CPS.

"Certificate" means a "Group Organization Certificate" as provided in for in the CPS, which are applied for by You in connection with this Agreement and which actually consists of two digital certificates, one the Group Organization Encryption Certificate and the other the Group Organization Signing Certificate, which are to be construed hereunder as a single digital certificate unless indicated otherwise through the use of the term " Group Organization Signing Certificate " or " Group Organization Encryption Certificate". Also, when "Certificate" is used herein, such use is to be constructed to include an "if issued" condition.

"Compromised" means a given Private Key is in danger of being lost, disclosed, or subjected to unauthorized use in any way.

"CP" means the most recent version of the *IdenTrust Global Common Certificate Policy* posted by IdenTrust to the Repository, which may be amended from time to time by IdenTrust in its sole discretion.

"CPS" means the most recent version of the *Certificate Practice Statement for IdenTrust Global Common Certificate Policy* posted by IdenTrust to the Repository, which may be amended from time to time by IdenTrust in its sole discretion.

"Cryptomodule" means hardware or software that: (i) generates Key Pairs; (ii) stores cryptographic information (such as the Private Key); and (iii) performs cryptographic functions.

"Digital Signature" means the transformation of an electronic record by one person using a Private Key and Public Key Cryptography so that another person having the transformed record and the corresponding Public Key can accurately determine: (a) whether the transformation was created using the Private Key that corresponds to the Public Key; and (b) whether the record has been altered since the transformation was made.

"Government Agency" means any government body or administrative unit of government of (a) the Federal Government of the United States of America or (b) any State among the United States of America; provided, however, no entity that is a corporation shall be considered a Governmental Agency.

"Human Sponsor" means a person designated as such in accordance with the Subscribing Organization Authorization Form or as provided under Section 15.

Health Domain Name: A Health Domain Name is a string conforming to the requirements of RFC 1034 and identifies the organization that assigns the Health Endpoint Names.

*Example: direct.sunnyfamilypractice.example.org. A Health Domain Name must be a fully qualified domain name, and should be dedicated solely to the purposes of health information exchange.*

Health Endpoint Name: A Health Endpoint Name is a string conforming to the local-part requirements of RFC 5322. Health Endpoint Names express real-world origination points and endpoints of health information exchange, as vouched for by the organization managing the Health Domain Name.

*Example: johndoe (referring to an individual), sunnyfamilypractice, memoriallab (referring to organizational inboxes), diseasesregistry (referring to a processing queue).*

"ID Form" means the ID Form completed and signed in connection herewith.

"Identity Certificate" means a Public-Key Cryptography certificate that provides authentication of the identity claimed by the certificate holder named in such certificate and create Digital Signatures.

"IdenTrust" means IdenTrust Services, LLC.

"IdenTrust Privacy Policy" means the then-current version of the Privacy Policy located at: [identrust.com/privacy.html](http://identrust.com/privacy.html)

"IGC Group Organization Certificate" has the meaning given "Certificate" herein.

"Key Pair" means two mathematically related Keys (a Private Key and its corresponding Public Key), having the properties that: (a) one Key can be used to encrypt a communication that can only be decrypted using the other Key; and (b) even knowing one Key it is computationally infeasible to discover the other Key.

"Operational Period" means the Certificate's actual term of validity, beginning with the start of the Validity Period and ending on the earlier of: (i) the end of the Validity Period disclosed in the Certificate; or (ii) the revocation of the Certificate.

"PKI Service Provider" has the meaning provided such term in the CPS.

"Private Key" means the key of a Key Pair kept secret by its holder and that can be used by its holder to encrypt or decrypt messages or to create a Digital Signature.

"Public Key" means the key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and that can be used by the holder to validate Digital Signatures created with the corresponding Private Key and to encrypt messages or files to be decrypted with the corresponding Private Key.

"Public Key Cryptography" means a form of cryptography (a process of creating and deciphering communications to keep them secure) in which two keys are used. One key encrypts a message, and the other key decrypts the message. One key, the Private Key, is kept secret, and the other, the Public Key, is made available to others. These keys are, in essence, large mathematically related numbers that form a unique pair. Either key may be used to encrypt a message, but only the other corresponding key may be used to decrypt the message.

"Registrar" has the meaning set forth in the CPS.

"Repository" means the information and data repository of IdenTrust located at the following address:

<https://secure.identrust.com/certificates/policy/igc/index.html>

"Relying Party" means any person or entity that in conformity with the CPS reasonably relies on the Certificate during its Validity Period.

"Subscribing Organization" shall mean the entity described as such in the Subscribing Organization Authorization Form completed and signed in connection herewith.

"Subscribing Organization Authorization Form" means the Subscribing Organization Authorization Form completed and signed in connection herewith.

"Validity Period" is the intended term of validity of a Certificate, beginning with the "notBefore" date asserted in the Certificate and ending with the "notAfter" date asserted in the Certificate.

"You" and "Your" refers to the non-human "Subscriber" of the Certificate. Such non-human Subscriber has Human Sponsor(s) each of whom is responsible for carrying out such non-human Subscriber's responsibilities.